CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 **FINAL DRAFT** CJCSI 6211.02B
DISTRIBUTION: A, B, C, J, S 2 April 2003

DEFENSE INFORMATION SYSTEMS NETWORK (DISN): POLICY, RESPONSIBILITIES AND PROCESSES

References(s): Enclosure D.

1. Purpose. This instruction establishes policy, responsibilities, and connection approval process for subnetworks of the Defense Information Systems Network (DISN). Additional overall and specific policies governing other subnetworks of the DISN are covered in the following instructions:

a. CJCSI 6250.01A, "Satellite Communications" (reference a).

b. CJCSI 6215.01B, "Policy for Department of Defense Voice Networks" (reference b).

c. Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartmented Information within Information Systems" (reference c).

2. Cancellation. CJCSI 6211.02A, 22 May 1996, "Defense Information System Network and Connected Systems," is cancelled.

3. Applicability. This instruction applies to the Joint Staff, Combatant Commands, Services, Defense Agencies, Department of Defense (DOD) field activities and joint activities; including DOD and Service Non-Appropriated Fund Instrumentalities.

4. Policy. Enclosure A

5. Definitions. See Glossary

6. Responsibilities. Enclosure B

7. Summary of Changes.

a. This new version focuses on DISN policy and responsibilities with additional emphasis on processes for secure connection of unclassified and classified information systems.

b. Provides guidance on the DISN Security Assurance Program.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/doctrine. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective immediately.

{NAME1}
{Rank1}
{Title1}

Enclosure(s):
A - Policy
B - Responsibilities
C – Connection Process
D - References
Glossary

68
69
70 DISTRIBUTION
71
72 Distribution A, B, C, and J plus the following:
73
74 ..... Copies
75
76 Secretary of Defense.....2
77 Secretary of State.....2
78 Director of Central Intelligence.....5
79 Assistant Secretary of Defense (Command, Control,
80 Communications and Intelligence).....5
81 Director, National Security Agency.....4
82 Director, Joint Interoperability Test Center.....2
83 Director, Inter-American Defense Board.....2
84 Chairman, US Section US-Canada Military
85 Cooperation Committee.....2
86
87
88

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-A-1 thru C-A-6	O
i thru viii	O	C-B-1 thru C-B-6	O
A-1 thru A-6	O	D-1 thru D-2	O
B-1 thru B-16	O	GL-1 thru GL-8	O
C-1 thru C-14	O		

(INTENTIONALLY BLANK)

187
188

189 RECORD OF CHANGES

190

Change No.	Date of Change	Date Entered	Name of Person Entering Change

191
192
193

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

POLICY

1. DISN Background

a. The DISN is DOD's worldwide network that allows the warfighter to exchange information in a seamless, interoperable, and global battlespace. Its underlying infrastructure is composed of three major segments or blocks:

(1) The sustaining base (i.e., base, post, camp, or station and Service Enterprise Networks) Command, Control, Communications, Computers and Intelligence (C4I) infrastructure that will interface with the long-haul network to support the deployed warfighter.

(2) The long-haul telecommunications infrastructure, which includes the communication systems and services between the fixed environment and the deployed joint task force (JTF) and/or coalition task force (CTF) warfighter.

(3) The deployed warfighter and associated Combatant Commander telecommunications infrastructures supporting the JTF and/or CTF.

b. The DISN infrastructure is an integrated network, centrally managed and configured to provide dedicated point-to-point, switched voice and data, and video services in support of national defense C4I decision support requirements.

c. The DISN provides the global transfer infrastructure by integrating separate Combatant Command, Service and Agency (C/S/A) networking requirements into a DOD enterprise-wide network to meet common-user and special purpose information transfer requirements.

d. DISN information transfer facilities support secure transmission requirements for subnetworks such as the Defense Switch Network (DSN), Defense Red Switch Network (DRSN), Non-classified Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS).

2. DISN Required Features

a. Global in scope.

b. Interoperable between all infrastructure segments or blocks.

c. Support multiple information transfer services for DOD users, including:

(1) dedicated point-to-point;

(2) switched voice and data, currently NIPRNET, and SIPRNET; and

(3) video services.

d. Capable of rapid expansion or reconfiguration (minutes and hours) and extension to the tactical environment, and be interoperable with tactical systems. Bandwidth capacity for surge will be engineered and allocated based on contingency requirements and Joint Staff validation and direction.

e. Support automatic rerouting and restoral of circuits by priority IAW with existing National Security Emergency Preparedness (NSEP) procedures, Telecommunications Service Priority (TSP) procedures, and other procedures as required to ensure network performance and user requirements are met.

f. Operation, maintenance, and management under the full control of military and DOD civilian personnel.

g. Robust, adaptive, and reliable by employing network and configuration management, diverse routing, and automatic rerouting features.

h. Subnetwork and component survivability commensurate with the supported command or mission.

i. Support multilevel precedence and preemption (to meet assured connectivity requirements) and all classifications of information.

j. Support value-added services, such as messaging and conferencing, and allow for the addition of new services and technologies.

k. Provide a secure information environment for the processing, storage, transfer, and use of information in accordance with the DISN security policy.

l. Capable of detecting attempts to access the network by unauthorized users. Support automatic denial of such access attempts and automated reporting of such attempts to the DISN management structure.

3. Policy

a. All DOD long-haul communications requirements will be submitted to Defense Information Systems Agency (DISA) in accordance with (IAW) DODI 4640.14 (reference d). DISA will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements. Sustaining base and deployable requirements will be processed IAW reference d and the supporting components' procedures.

b. All connections will follow connection approval procedures and processes, as established in this instruction. This includes requests for cross-domain connection of TOP SECRET, Special Access Program (SAP) or Special Access Requirement (SAR) information systems or networks either directly or indirectly to the SIPRNET.

c. Connections must be designed, developed, integrated, certified and accredited as part of the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) and documented in a System Security Authorization Agreement (SSAA) IAW DOD Directive 8500.1 (reference e) and DOD Instruction 5200.40 (reference f) and DOD 8510.1-M (reference g).

d. Secure configurations of approved information assurance (IA) and IA-enabled information technology (IT) products, uniform risk criteria, trained systems security personnel, and strict configuration control will be used for DISN.

e. The community risk will be assessed and measures taken to mitigate risk IAW procedures established by the DISN Designated Approving Authorities (DAAs).

(1) Applications or systems that will be deployed to multiple enclaves connected to the long-haul infrastructure will be assessed for security features and community risk.

(2) Applications or systems that have not completed assessments may only be deployed on operational networks with specific site and DISN DAA approval. Such deployments will be of limited duration and develop operational usage guidelines and procedures.

f. All connections of information systems will be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

g. Information provided through connections must be released IAW DOD 5200.1-R (reference h), DOD Directive 5230.11 (reference i), and CJCSI 5221.01 (reference j).

h. Connection among information systems of different security domains (e.g., different classification levels, formal compartments, DOD with non-DOD entities) will be IAW DOD Directive 8500.1 (reference e) and DOD Instruction 8500.2 (reference k). As a condition of approval, such devices must have an identified program management structure that retains configuration management responsibility for all deployed systems throughout their operational life-cycle.

(1) Connections among DOD information systems of different security domains or with other Non-DOD US Government systems of different security domains will be used only to meet compelling operational requirements, not convenience.

(2) The connection of DOD information systems with those of US allies, foreign nations, coalition partners, or international organizations must be approved by the DISN DAAs, follow applicable international agreements, DOD Directive 8500.1 (reference e) and CJCSI 6510.01 (reference l).

(3) The connection of TOP SECRET, SAP or SAR information systems to the SIPRNET must be approved by the DISN DAAs and comply with applicable security directives and instructions.

(4) Cross-domain connections will be reviewed annually to ensure a valid operational requirement for the connection still exists and the current implementation satisfies the requirement. Because these connections are considered high risk, they will be recertified annually and reaccredited every 3 years. Recertification will include an independent vulnerability assessment of the connection (i.e., assessment by organization not directly responsible for connection).

(5) Only cross-domain solutions (i.e., process limiting the exchange of information between systems) approved by the DISN DAAs may be used to connect information systems of different security domains.

(6) Procedures within the DITSCAP process, including registration with the Global Information Grid (GIG) Interconnection Approval Process (GIAP) office, review of connections as part of the GIAP and community-wide risk assessment by Cross-Domain Technical Advisory Board (CDTAB) for approval by the DISN Security Accreditation Working Group (DSAWG) must be followed.

(7) The four DISN DAAs (Director, Joint Staff; Director, DISA; Director, Defense Intelligence Agency (DIA); and Director, National Security Agency (NSA)) hold the responsibility for reviewing and accepting the risk of operating the DISN and all connected systems (DOD Directive 8500.1 (reference e).

i. Connections between DOD and Non-DOD government information systems will comply with DODI 5200.40 (reference f) or equivalent document.

j. Connections between DOD and contractor information systems will comply with DODI 5200.40 (reference f) or equivalent document.

k. Connected systems and enclaves will be supported by an inspection/site visit program to meet security requirements. This program links existing inspection and site assistance/visit actions to support the DISN DAAs accreditation decisions of DISN components and user enclave connections (reference f, Phase IV).

(1) All enclaves connected to the DISN long-haul are subject to compliance inspections.

(2) All enclaves connected to the DISN long-haul are subject to electronic monitoring for communications management and network security purposes.

l. All DOD personnel are personally and individually responsible for providing proper protection to classified information under their custody and control, including information on their information systems and networks. All officials within the DOD who hold command, management (e.g., DAA and Information Assurance Manager (IAM)), or supervisory positions (e.g., Information Assurance Officer (IAO) or supervisors) have specific, responsibility for the implementation and management quality of the Information Security Program within their areas of responsibility (DOD 5200.1-R (reference h)).

m. The DISN will be used for official and authorized purposes only.

(1) This includes emergency communications and any other communications that the Combatant Commands determines are necessary in the interest of DOD. In the interest of morale and welfare, Combatant Commanders may approve communications by DOD employees and military members to their family members at home from locations to which they are deployed for extended periods of time on official business.

(2) Authorized purposes include, for example, brief communications made by military members and DOD employees during official travel to notify family members of transportation or schedule changes. Reasonable personal communications (such as auto or home repair appointments or brief Internet searches) from the military member or DOD employee at his or her workplace are also authorized when the C/S/A permits categories of such communication and after determining that such communications:

(a) Do not adversely affect the DOD organization's performance or military member's or DOD employee's official duties.

(b) Are of reasonable duration and frequency, and whenever possible, made during the employee's or military member's personal time such as after normal duty hours or during lunch periods.

(c) Serve a legitimate public interest, such as enabling DOD employees or military members to stay at their desks rather than requiring them to depart the work area to use commercial systems, or improving the morale of military members and DOD employees stationed away from home for extended periods of time.

(d) Would not reflect adversely on DOD (e.g., pornography, chain letters, unofficial advertising or soliciting, inappropriate handling of classified information)

(e) Do not overburden the communication system and create no significant additional cost to DOD.

n. DISN non-Defense Satellite Communication System costs will be recovered through the Defense Business Operating Fund (DBOF) Communication Information Services Activity (CISA) through a billing scheme that is published by DISA. Non-DOD activities will be billed through the respective C/S/A approval authority.

o. Survivability enhancements in transmission paths, routing, equipment and associated facilities will normally be limited to systems supporting critical missions that justify additional costs.

ENCLOSURE B

RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff (CJCS) is responsible for operational network policy and overall direction of the DISN.

a. The Director, Joint Staff delegates to the Director for Command, Control, Communications, and Computer Systems (J-6) authority for operational DISN policy and direction.

b. The Director for Command, Control, Communications, and Computer Systems (J-6), will:

(1) Serve as one of the DISN DAAs and exercise authority for operational DISN policy and direction.

(2) Appoint a flag-level representative to the DISN Flag Panel.

(3) Appoint an O-6/GS-15 representative to the DSAWG.

(4) Monitor the operational and management effectiveness of the network and report significant items (e.g., major mission degradation) to the CJCS.

(5) Resolve DISN requirement conflicts and issues referred to the Joint Staff or through the Military Communications Electronics Board (MCEB) as appropriate.

(6) Develop Joint policy, responsibilities, and connection process for DISN. Integrate lessons learned from Information Assurance Panel and DSAWG.

(7) Coordinate assignment of funding responsibility for joint requirements to the appropriate Service.

(8) Validate operational requirement of Non-DOD government and contractor connections.

(9) Validate and approve operational requirement of all cross-domain connections including combatant command endorsed requests for foreign entity connections.

(10) Direct Joint Vulnerability Assessment Process (JVAP) visits, as required.

(11) Issue disconnection notices as approved by the DISN DAAs.

2. The Combatant Commanders, in addition to responsibilities in subparagraph 9, will:

a. Submit their validated DISN requirements through Service channels to DISA. Commander, US Special Operations Command will submit service requirements directly to OSD.

b. Review and submit service restoration priority requests IAW with DISA Circular 310-130-4 (reference m).

c. Endorse foreign entity connection requests and forward request through the Joint Staff, J-6 (validation) to the Assistant Secretary of Defense for Command, Control, Communications (ASD(C3)) for approval.

3. The Commander, US Strategic Command (USSTRATCOM), in addition to responsibilities in subparagraph 2 and 9 will: Appoint in writing an O-6/GS-15 representative to the DSAWG.

4. The Services Chiefs, in addition to responsibilities in subparagraph 9, will:

a. Appoint an O-6/GS-15 representative to the DSAWG.

b. Coordinate cross-domain connections through their Cross-Domain Solutions Organizations.

c. Provide local data distribution capability to meet Combatant Command validated connectivity requirements. (These systems must be focused on supporting operational requirements of the parent Service and be capable of supporting contingency operations (e.g., joint task force headquarters)).

d. Appoint an O-5/GS-14 representative to the CDTAB. Formerly known as the SECRET and Below Interoperability (SABI) PAT.

e. Establish Cross-Domain Solution Offices to validate and prioritize requests.

f. Provide requisite site support for the DISN equipment located on their respective bases, posts, camps and stations. Site support will be specified by DISA in appropriate procedural documentation and

coordinated with the Service.

5. The Director, DISA, in addition to responsibilities in subparagraph 9, will:

a. Serve as the DISN network manager.

b. Serve as one of the four DISN DAAs.

c. Appoint a flag-level representative to the DISN Flag Panel.

d. Appoint an O-6/GS-15 as chairperson of the DSWAG.

e. Appoint an O-6/GS-15 representative to the DSAWG.

f. Appoint an O-5/GS-14 as co-chair person of the CDTAB.

g. Appoint an O-5/GS-14 as representative to CDTAB.

h. Assess the technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN. New services and capabilities will be added in response to validated user requirements and planned technology insertion.

i. Provide final approval for all DISN connections ensuring operational requirements have been validated; connections meet all technical and interoperability requirements; and subnetworks, systems, and other connected components provide adequate security and have been accredited by the proper authority.

j. Develop, coordinate, and publish DISN connection criteria in conjunction with Services and Defense Agencies.

k. Provide operational management for the DISN and be responsive to the validated operational requirements of the Joint Staff and C/S/As.

l. Establish a management structure for the DISN and exercise operational direction to include:

(1) Conduct day-to-day network management of the DISN.

(2) Maintain configuration management of the DISN (e.g., maintaining an accurate and appropriately classified data base of existing DISN users, including non-DOD activities, and monitoring system service restoration).

m. Monitor the effectiveness of the DISN-provided services in satisfying user requirements and respond to Combatant Command requests for reports on system performance.

n. Perform required system engineering and modeling to achieve optimal network design and implementation approach, and identify performance standards for DISN services (e.g., availability and response time).

o. Refer to the Joint Staff any matters that significantly degrade the network.

p. Provide Joint Staff, C/S/As appropriate periodic status and programmatic updates.

q. Analyze and satisfy requests for new DISN services in coordination with the Joint Staff and appropriate C/S/As.

r. Specify and maintain (GIAP web site http://giap.disa.smil.mil//) interoperable interface protocol standards, in coordination with the C/S/As.

s. Chair the DSAWG on all DISN connection requests.

t. Ensure the DISN security architecture meets the needs of the DISN users.

u. Develop and maintain DISN planning and program management process and documentation.

v. Ensure security measures, plans, and accreditation policies are based on threat assessments validated by the appropriate member(s) of the DOD Community.

w. Provide qualified personnel to conduct compliance with connection requirements, assistance and correction, and technical assessments.

x. Advise the CJCS and Commander, USSTRATCOM on the allocation of DISN resources and network anomalies.

y. Support the Combatant Commands in creating a network common operational picture (COP) for their area of responsibility (AOR).

z. Coordinate the provisioning of network services across the transport network, IAW CJCS and Combatant Command requirements. As such, DISA will serve as the single point of contact for C/S/A DISN

managers when they require service continuity across multiple transport networks.

aa. Lead technical efforts related to the end-to-end integration and capability of GIG networks to include testing support, interoperability certification, and joint spectrum management.

bb. Provide support to the DOD Chief Information Officer (CIO), the Joint Staff, Joint Forces Command, and other Combatant Commands to achieve GIG network interoperability.

cc. Support NSA development of the overall community cross-domain solution architecture.

dd. Establish the SIPRNET Connection Approval Office (SCAO) which will:

(1) Serve as primary coordinator to process and review DOD requests for connection of classified security domains, including, but not limited too, the SIPRNET.

(2) Coordinate and jointly manage, with NSA, implementation of the GIAP for connection requests, and ensure feedback between supporting organizations and the DOD Components.

(3) Approve requests that are DOD only, single level connections.

(4) Implement all approved connection requests.

(5) In coordination with NSA, develop and maintain a SIPRNET connection manual describing the step-by-step process the requestor will follow to request and implement a cross-domain connection.

(6) Develop and maintain the GIAP-Classified Systems database and web site for recording the technical and operational characteristics of all active connections between different security domains.

(7) Coordinate with NSA in maintaining SSAA guidance and templates posted to the GIAP website (http://giap.disa.smil.mil//) for use by the customer.

(8) In coordination with NSA, identify vulnerabilities, configuration or operational changes that affect individual or classes of accredited cross-domain connection implementations; notify the DSAWG and affected DAAs of such changes.

(9) Develop, in coordination with NSA, the JVAP to insure all cross-domain connections are assessed on an annual basis.

(10) Ensure through the coordination with site DAAs (e.g., base, camp, post or station) that cross-domain connections are re-accredited annually, to include penetration testing, vulnerability and risk assessment, using the Risk Decision Authority Criteria. The DISA SCAO will monitor open vulnerabilities to insure compliance.

(11) In coordination with NSA, develop and implement a network security education, training and awareness program.

(12) Assist the DOD Components in integrating the cross-domain connection process into their certification and accreditation and configuration management activities.

(13) Provide, in coordination with NSA, semi-annual status reports on cross-domain connections (CJCSI 6510.01, reference l) to the DOD CIO, the CJCS, and the C/S/As and their DAAs with active or planned cross-domain connections.

ee. Establish the GIAP-Unclassified Systems connection approval office which will:

(1) Implement all approved connection requests.

(2) Review all commercial Internet Waiver requests to DOD systems (network and stand alone).

ff. Perform SIPRNET and NIPRNET Compliance Validation visits to potential high-risk (e.g., cross-domain) connections. Reports of these visits will be maintained on the DISA/Field Security Office Vulnerability Management System (VMS) database.

(1) Reports will be available for selective reviews by the DISN DAA and C/S/As.

(2) Inspected sites can respond to Compliance Visit open findings via VMS.

(3) Compliance validation visits will consist of traditional security checks, scanning (automated tool) of the connected network, and a JVAP if a device is operational. Compliance validation visit checklists can be downloaded at web site http://guides.ritchie.disa.mil.

(4) DISA teams will assess the security implementation on the connected environment from the cryptographic device down to the workstation for the SIPRNET connections and from the point of presence of the connection to the servers for the NIPRNET connections.

6. The Director, DIA, in addition to responsibilities in subparagraph 9 will:

a. Serve as one of the four DISN DAAs.

b. Appoint a flag-level representative to the DISN Flag Panel.

c. Appoint an O-6/GS-15 representative to the DSAWG.

d. Implement, operate and manage JWICS components and facilities on the DISN IAW established agreements with DISA.

e. Provide threat data to support the risk assessments and decisions on cross-domain connections.

7. The Director, NSA, in addition to responsibilities in subparagraph 9 will:

a. Serve as one of the four DISN DAAs.

b. Appoint a flag-level representative to the DISN Flag Panel.

c. Appoint an O-6/GS-15 representative to the DSAWG.

d. Appoint an O-5/GS-14 as co-chair person of the CDTAB.

e. Appoint a JVAP representative.

f. Provide guidance on required security services and features necessary to meet DISN operational requirements.

g. Recommend techniques and procedures to minimize DISN information security vulnerabilities IAW DODD 8500.1 (reference e) and Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01 (reference n).

h. Develop and/or certify communications security (COMSEC) solution. Produce keying material for all COMSEC.

i. Establish a TOP SECRET and Below Interoperability (TSABI) Program Office to support the Intelligence Community (IC) in implementing the TSABI process for TOP SECRET/Sensitive

Compartmented Information (S_C_I) information systems to systems of different security domains.

j. Establish the NSA Cross-Domain Solutions Organization (CDSO) in support of DOD and IC connection requirements, to include:

(1) Manage the community wide information systems security engineering (ISSE) process for the design, development, integration, testing (laboratory and on-site testing), and solution documentation for validated connection requests.

(2) Develop and maintain (http://www.iad.nsa.smil.mil) the Risk Decision Authority Criteria for identifying an acceptable level of community risk appropriate for the connection approval authorities to use in making connection decisions.

(3) Develop the overall community cross-domain solution architecture in coordination with DISA and the DOD Service and Agency solution developers.

(4) Develop and maintain (http://www.iad.nsa.smil.mil) Protection Profiles for cross-domain solutions in accordance with the Common Criteria.

(5) Act as the type-certification authority for cross-domain solutions (e.g., guards).

(6) Develop, maintain, and oversee a common DOD and IC process for cross-domain solution development, to include specification of robustness and evaluation standards.

(7) Approve the security criteria for new cross-domain components.

(8) Develop and maintain (http://www.iad.nsa.smil.mil) a RI listing of recommended, type-certified, connection security implementations. Each RI will include guidance for appropriate use including security concept of operations. Provide sample SSAA for DSAWG approved technology to assist and expedite the accreditation process.

(9) In coordination with C/S/A cross-domain solutions organizations, support site personnel and system developers to adapt existing RIs to the specific environment. The NSA CDSO will review the resulting cross-domain architecture, and ensure the resulting solution is

consistent with the overall cross-domain solution architecture.

(10) In coordination through C/S/A cross-domain solutions organizations, support site personnel, the DISA SCAO, and system developers to engineer new cross-domain solutions for requirements not adequately addressed by existing RIs. The NSA CDSO will review the resulting cross-domain architecture, and ensure the resulting solution is consistent with the overall cross-domain solution architecture.

(11) Identify vulnerabilities that affect individual or classes of accredited connection implementations. Coordinate with DISA on notification of C/S/As and site DAAs for affected systems.

(12) In coordination with C/S/A cross-domain solutions organizations, assist the site DAA in performing the local risk assessment and provide feedback to the DAA in completing their SSAA for the connection implementation.

(13) Support DISA development of a SIPRNET connection manual describing the step-by-step process the requestor will follow to request and implement a connection between classified security domains.

(14) Serve as the community certification authority and make recommendations to the DSAWG and the DISN DAAs on the connection implementations for community networks.

(15) Provide technical support to DISA for development and conduct of a cross-domain JVAP.

(16) Support DISA development of semi-annual status cross-domain connections reports to DOD CIO, CJCS, and C/S/As and their DAAs with active or planned cross-domain connections.

8. The Director, Defense Security Service (DSS) in addition to responsibilities in subparagraph 9 will:

a. Appoint a DAA for contractor connections to DISN.

b. Establish security requirements for contractor DISN connections and connected enclaves.

c. Conduct compliance inspections and assistance visits of contractor connections/enclaves and direct correction of any deficiencies.

9. C/S/As, DOD Field Activities and Joint Activities will:

a. Review long-haul common-user transmission requirements and forward all requirements not needing Combatant Command, the Joint Staff, or ASD(C3) validation and approval to DISA for development of technical solution, coordination and implementation.

b. Identify to DISA each DOD system or application device having a requirement for long-haul common-user information transfer services for DISN planning purposes. Systems and requirements will be identified to DISA as soon as requirements for these services are validated.

c. Assess technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN in regards to the sustaining base and deployable infrastructure. New services and capabilities will be added in response to validated user requirements and planned technology insertion in coordination with DISA.

d. Coordinate Service and Defense Agency long-haul requirements for DISN access within a Combatant Commander's geographic AOR with Combatant commander and DISA prior to submission.

e. Validate the requirement and maintain oversight for all component connections.

f. Program, budget, fund and provide support for assigned portions of the DISN, including for connection solution(s) (e.g., guards) development, procurement, operation and maintenance.

g. Manage DISN subnetworks when authorized by the Director, J-6, the Joint Staff.

h. Document and validate the operational and IA requirements for the connection.

i. Prior to developing a cross-domain solution, require program offices or other developers to coordinate the solution development with the NSA CDSO.

j. Ensure foreign entity connection requests are endorsed by a combatant command and forwarded for validation and approval by the Joint Staff (J-6).

k. Ensure non-DOD (e.g., contractor, other USG agency or organization) connection requests are endorsed (i.e., sponsored) by a DOD organization and forwarded for validation by Joint Staff (J-6) and approval by ASD(C3).

l. Apply applicable information, communications, and physical security measures and ensure installation requirements continue to meet the requirements of the DISN security policy.

m. Ensure approved systems use DISN services to meet mission requirements.

n. Ensure user compliance with DISN policy and procedures.

o. Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits according to DISA-established criteria.

p. Provide information, as requested, to DISA for DISN billing, management and inventory purposes.

q. Conduct compliance inspections, assistance visits, technical engineering inspections, and remote monitoring and vulnerability assessments of DISN connections and the connected enclaves in support of DISN Assurance Program.

r. Establish procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, or determination that cross-domain connections may put classified information at risk of compromise IAW DOD 5200.1-R (reference h).

(1) Actions will focus on correction or elimination of the conditions that caused or occasioned the incident.

(2) Incidents will be reported IAW DOD 5200.1-R (reference h).

(3) Military and civilian personnel will be subject to sanctions if they knowingly, willfully, or negligently compromise or put classified information at risk of compromise. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law.

10. The DISN DAAs, will:

a. Serve as the final approval authority for DISN connections and operations after a full evaluation by NSA and DISA of the connection and

cross-domain technology has been conducted.

b. Appoint DISN Flag Panel members.

c. Delegate in writing approval authority to the Flag Panel, DSAWG and/or DISA SCAO for specific type requests.

d. Assess and manage the risk of operating all connected systems within the DISN.

e. Serve as the approving authority for all DOD classified cross-domain solutions submitted by C/S/As.

f. Serve as the final appeal for connection requests. Unanimous approval by DISN DAAs required for connection.

g. Make final determination, with DSAWG and Flag Panel recommendation, to disconnect or disapprove a cross-domain connection or cross-domain solution (see figure C-1).

h. Annually review cross-domain connections. Because these connections are considered high risk, they will be reaccredited annually, and re-certification of the connection will include a JVAP.

11. DISN Flag Panel will:

a. Support the DISN DAAs in their role as final approval authority for all DISN connections and cross-domain solutions.

b. Make connection approval decisions for those classes of systems and circumstances delegated by the DISN DAAs.

c. Review and adjudicate DSAWG recommendation(s) on connections involving new technology, high risk, or foreign nationals and make recommendations to the DISN DAAs for the disconnection or disapproval of a cross-domain solution.

d. Review appeals from connection sponsors of DSAWG decisions. Support the DISN DAAs in their annual review of operational connections.

12. DISN Security Accreditation Working Group (DSAWG) will:

a. Support DISN DAA's in their role as final approval authority for all DISN connections.

b. Make connection approval recommendations to the Flag Panel and DISN DAA's.

c. Make connection approval decisions for those classes of systems and circumstances delegated by the DISN DAAs (e.g., similar architectures and cross-domain systems previously approved by DISN DAAs).

d. Make recommendations to the Flag Panel and DISN DAAs for the disconnection or disapproval of a cross-domain solution.

e. Develop and coordinate the approval of the DISN Security Policy.

f. Guide or assist development of DISN integrated system/security architecture and policy changes.

g. Provide the DOD community risk assessment for all cross-domain connections between classified domains including, but not limited to, connections to the DISN.

h. Provide early assessment of risk to the DISN Flag Panel.

i. Coordinate with the Defense and Intelligence Community Accreditation Support Team (DICAST) and the IC Information Assurance Policy Board (IAPB) on all cross-domain connections between TOP_SECRET/S_C_I and other DOD classified domains including, but not limited to, connections to the DISN.

j. Monitor life cycle of the DISN long-haul Service to identify and resolve security issues.

k. Make DISN connection accreditation policy recommendations to the MCEB.

l. Make recommendations to the DISN Flag Panel on resource prioritization for DISN connection requests.

m. Provide security assessments to the GIG Waiver Review Panel in support of the DOD CIO GIG Waiver Process. Note: The GIG Waiver Review Panel supports the DOD CIO Executive Board for Requests for Waiver of the DISN.

13. The Cross-Domain Technical Advisory Board (CDTAB) will:

a. Act as an advisory board to the DSAWG.

b. Perform technical risk assessments of cross-domain solutions.

c. Report results of the assessments (and possible alternative proposals to mitigate risk) to the DSAWG.

d. Operate under the direct guidance of the DSAWG and the general guidance of the Flag Panel.

14. Enclave or Site DAAs will execute the following responsibilities for connection to DISN:

a. Ensure compliance with the GIAP process.

b. Identify and inform other DAAs affected by the connection and assist in developing the associated community risk assessment.

c. Ensure local risk assessment of each connection implementation is conducted to determine whether the local level of risk is acceptable. Develop and implement the SSAA to maintain configuration control of the connection.

d. Ensure review of all cross-domain connections annually to ensure valid operational requirement still exists and the current implementation satisfies the requirement.

e. Ensure connections between security domains are recertified annually and reaccredited every 3 years, to include penetration testing, vulnerability and risk assessment.

f. Ensure a properly conducted certification is accomplished on each system considered for accreditation IAW DITSCAP.

g. Grant final and interim accreditation of a network or system.

h. Verify that each SSAA complies with information system security requirements as reported by the IAM. Ensure the operational information systems security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.

i. Ensure records are maintained for all existing information system accreditations or certifications under the DAA's purview.

j. Request DSAWG approval for additional security mechanisms and software (e.g., encryption and guards) necessary for DISN connection and

comply with connection procedures.

k. Ensure when classified or sensitive information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as encryption or protected distribution systems (PDS) (see National Security Telecommunications and Information Systems Security Instruction (NSTISSI 7003, reference o).

15. Information Assurance Manager (IAM) will carry out responsibilities outlined in CJCSM 6510.01 (reference n). Note: The term IAM is interchangeably with the IA title Information Systems Security Manager (ISSM).

16. Information Assurance Officer (IAO) will carry out responsibilities outlined in CJCSM 6510.01 (reference n) and support the JVAP. Note: The term IAO may be used interchangeably with other IA titles (e.g., Information Systems Security Officer (ISSO), Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

17. Program Manager for multi-site/multi user application or system will identify security features for centrally developed systems.

18. Cross-Domain Solution Program Manager will maintain life-cycle configuration.

(INTENTIONALLY BLANK)

ENCLOSURE C

CONNECTION PROCESS

1. Connection Request uses language from the perspective of a site initiating the request. While sites will always be the ultimate location of this technology development work, prior to fielding to multiple sites, this development work may be accomplished via Service and Agency program efforts. In such cases, in compliance with reference f, those program offices will follow this process to achieve type accreditation status if their product relies upon cross-domain technology.

2. SIPRNET Connection Requests (See Figure C-1)

a. Step 0: Prepare Request

(1) In preparation for connection registration, organization having connection requirement will:

(a) Determine and document the mission needs the connection will support.

(b) Document the implementation information protection requirements and have the protection requirements validated. C/S/As solution providers may assist in the documentation of protection requirements. Implementation information protection requirements will include:

1. Information types and classifications.

2. Type of user access required.

3. Applicable policy.

4. Characterization of threats to the information types and classifications (types and characterization of adversaries, adversary attack types and motivations).

5. Required security services and strengths.

(c) DAAs representing the security domains to be connected will validate the implementation-independent information protection

requirements.

1. Single DAA will: Validate the protection requirements for the connected domains, if the security domains to be connected are under a single DAA with no DISN managed connectivity.

2. Multiple DAAs will: Validate the protection requirements for the connected domains, if the security domains to be connected involve more than one DAA but no DISN managed connectivity.

3. DISN DAAs will: Validate the protection requirements for the connected community, if the security domains to be connected involve any DISN managed connectivity.

4. Site or Enterprise DAA. The DAA requesting connection will validate the protection requirements for his domain.

(d) The DAA requesting must ensure there is a valid operational requirement for all connections.

b. Step 1 – Authorize and Prioritize Request

(1) Requests for single-level SIPRNET connection for DOD organization are validated by requesting DAA and submitted to GIAP under Step 2 below.

(2) Requests for cross-domain connection requirement of US classified or unclassified enclaves/networks to SIPRNET must be endorsed by the appropriate C/S/A headquarters, validated and meet requirements outlined in Appendix A prior to or simultaneously with submitting connection requirement under Step 2 below.

(3) Requests for SIPRNET connections for Non-DOD US government organizations, contractors and foreign entities must be validated and meet requirements outlined in Appendix A prior to or simultaneously with submitting connection requirement under Step 2 below.

(4) C/S/A will: Validate and prioritize their cross-domain connection requests and update prioritization whenever new requests are submitted.

(5) Joint Staff, J-6 will: Prioritize and provide guidance to NSA and DISA on cross-domain connection requests in coordination with the Joint Staff, J-3 in the event of operational priority conflicts or resource

constraints.

c. Step 2: Process Request

(1) DAA Requesting Connection of Enclaves will: Submit connection request through GIAP. The GIAP is a DISA SCAO managed web based process to initiate, guide and track connection requests.

(2) DISA SCAO will:

(a) Ensure appropriate validation of each request.

(b) Determine type of connection request.

1. Routine connection – Single level connection (enclaves of like security domains).

2. Cross-domain connection (different security domains) or high-risk connection.

(c) Assign ticket number and tracks requests throughout process.

(d) Direct request to appropriate engineering or connection approval process.

1. Routine connection – request forwarded to SIPRNET Connection Approval Process (SIPRCAP) for connection.

2. Cross-domain connection – request forwarded to NSA CDSO for tailoring of RI or development of new cross-domain solution.

(3) Determine the accreditation status of the enclaves before certifying the connection.

d. Step 3: Develop Connection Solution

(1) NSA CDSO will:

(a) Review the connection requests sent by the DISA SCAO.

(b) Verify the DISA SCAO assigned the appropriate connection type.

1. Appropriate Reference Implementation Exists: Connection of different security domains where the appropriate RI exists.

2. No Appropriate RI Exists: Connection of different security domains where appropriate RI does not exist.

(c) If the Appropriate RI exists, the NSA CDSO will:

1. Work with the site point of contact (POC) and appropriate C/S/A solution providers to adapt existing RI to the specific requirement.

2. Ensure the resulting solution is consistent with the overall community (i.e., DOD and IC) cross-domain architecture.

3. Approve the engineering documentation and implementation of the adapted solution.

(d) If no Appropriate RI exists, the NSA CDSO will:

1. Work with the site POC, the DISA SCAO and appropriate C/S/A developers to engineer a new solution.

2. Lead the security engineering effort to:

a Ensure the resulting solution is consistent with the overall community cross-domain architecture.

b Approve the development of new cross-domain components.

c Ensure the organization security evaluation criteria reflect the desired security functions and attributes.

e. Step 4: Evaluate Connection Solution

(1) NSA CDSO will:

(a) Facilitate the community security evaluation organizations (e.g. DISA, NSA, and DIA) in performing security evaluations and risk assessments of cross-domain solutions.

(b) Ensure security components meet the security criteria (ensure organization evaluation).

(c) Ensure RIs meet their security criteria (ensure RI evaluation).

(d) Ensure fielded solutions meet their security criteria.

(2) Community security evaluation organizations will: Perform security evaluations and risk assessments of the cross-domain solutions, as part of the CDTAB, in coordination with the NSA CDSO.

(3) Cross-Domain Technical Advisory Board (CDTAB) will:

(a) Review security evaluations and risk assessments.

(b) Forward connection recommendations to the appropriate approval bodies (DSAWG, Flag Panel, and DISN DAAs) through the DISA SCAO.

f. Step 5: Connection Approval

(1) DISA SCAO will:

(a) Review the entire request and other related documentation and provide guidance to the connection approval authorities.

(b) Document the accreditation status of the enclave on both sides of the connection.

(2) Single DAA will: Accredit the connection and notify the DISA SCAO through the GIAP, if the security domains of the interconnected systems are under a single DAA with no DISN connectivity.

(3) Multiple DAAs will: Accredit the connection and notify the DISA SCAO through the GIAP, if the security domains involve more than one DAA but no DISN managed connectivity.

(4) DISN DAAs will:

(a) Accredit the connection of the enclave to the long-haul transport infrastructure, if the security domains involve DISN managed connectivity. The local DAA accredits the enclave being connected.

(b) Delegate authority to the Flag Panel, DSAWG or DISA SCAO for some connection decisions. The DISN DAAs remain the decision authority for those connections not delegated.

(5) DSAWG will: Review and approve connections (as delegated) or forward recommendation(s) to the Flag Panel.

(6) Flag Panel will: Approve the connections (as delegated) or forward recommendation(s) to DISN DAAs for final resolution.

g. Step 6: Connection

(1) DISN DAAs, Flag Panel or DSAWG will. Provide connection approval or disapproval is provided to the DISA SCAO.

(2) DISA SCAO will:

(a) Notify the site and C/S/A DAA of approval with the results and conditions (including time limits) via an interim authority to connect (IATC) or an authority to connect (ATC) letter.

(b) Notify the site and appropriate C/S/A DAA of disapproval.

(c) Initiate disconnection process (Step 7) if a connection is identified as non-compliant with its IATC or ATC.

(3) Site DAAs will: Operate the approved enclave connection in compliance with approved conditions provided by DISA SCAO via IATC or ATC letter.

(4) DISA and NSA will:

(a) Review cross-domain connections annually to ensure a valid operational requirement for the connection still exists and the current implementation satisfies the requirement.

(b) Re-accredit connections considered high risk annually. Re-accreditation of the high-risk connections will include a JVAP. On-site JVAP is conducted annually, or as directed by the Joint Staff.

h. Step 7: Disconnection

(1) DISA SCAO will:

(a) Inform the DISN Flag Panel via the DSAWG of site non-compliance.

(b) Notify the site and the appropriate C/S/A representative.

(c) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the DISA SCAO advises the J6, Joint Staff.

(2) Flag Panel will: Recommend to Joint Staff/J6 that a disconnect warning notice be issued.

(3) Joint Staff, J-6 will:

(a) Initiate coordination with J3 and enclave component to assess operational impact of the potential disconnects.

(b) Release a message giving 30 days to bring the connection into compliance or submit a plan to achieve connection compliance. Submitted plan must lead to compliance within 60 days of notification message release.

(c) Issue a coordinated DISN DAA order to disconnect, if compliance is not achieved within 30 day or 60 day windows.

(4) DISA Network Operators will: Verify and implement disconnection as directed.

(5) Site DAA will:

(a) Disconnect device with approval from his/her senior headquarters, if DAA determines any device in the enclave, including cross-domain solution, is no longer required. The DAA will notify the DISA SCAO via letter and update the site SSAA.

(b) Terminate connection, if DAA determines that a connection is no longer required and notify the DISA SCAO via routine letter/message.

i. Timelines for Cross-Domain SIPRNET Connection Requirements

(1) Joint Staff, J-6 and ASD(C3) will:

(a) Validate and approve operational requirement for cross-domain connection requests (DOD different classification levels, Non-DOD government, contractor and foreign entities) within 5 working days, if all required information is provided by requesting/endorsing DOD organization.

(b) Validate and approve operational requirement for "CRITICAL" connection requests can be completed in 24 hours, if all required information is provided by requesting/endorsing DOD

organization.

(2) DISA SCAO will assign tracking number with 2 working days.

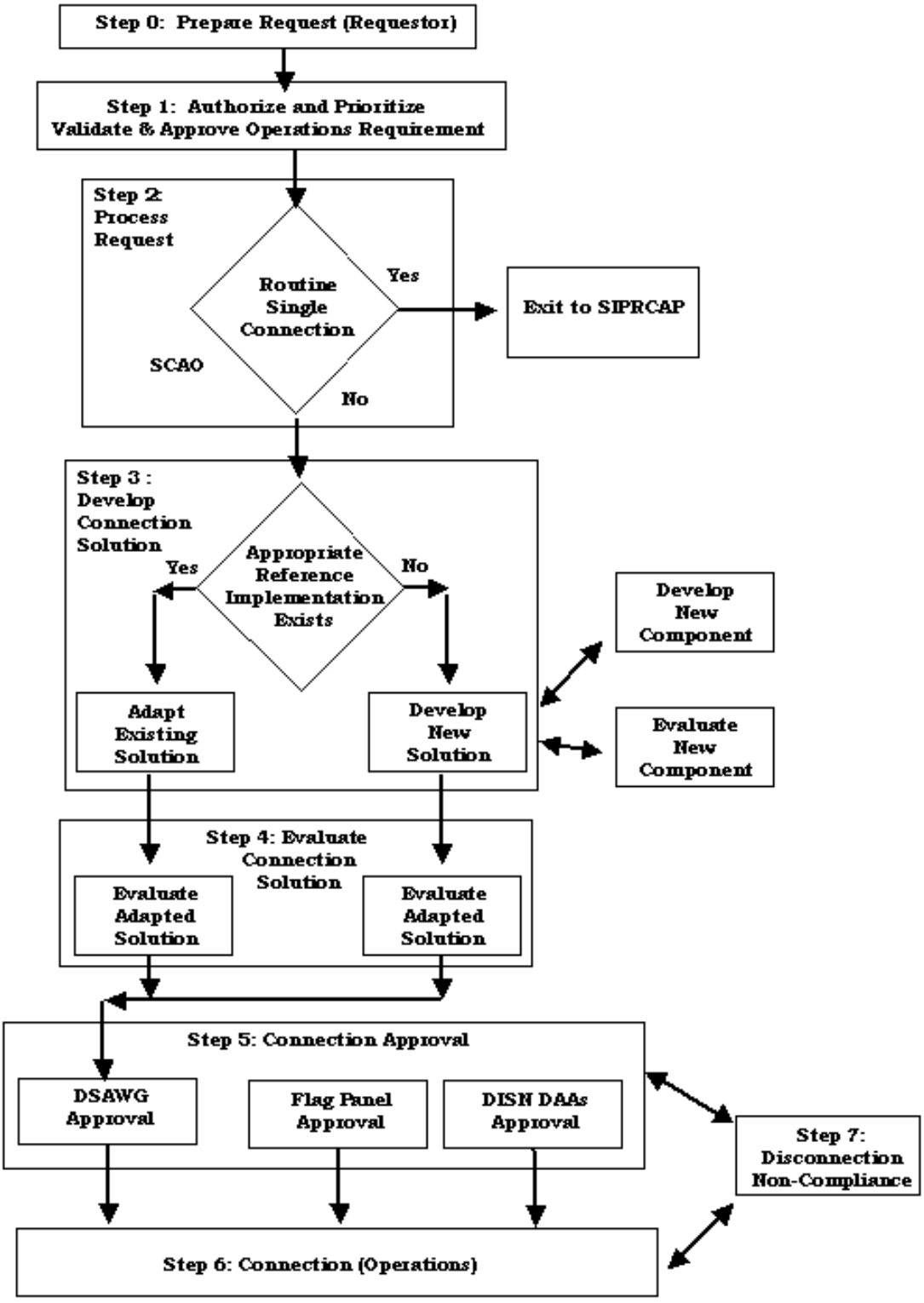
(3) NSA will:

(a) Complete engineering and evaluation (Step 2 and 3) within 4-6 weeks for connection requirements using existing connection solution requiring only tailoring of RI. Actual timelines for completion will depend on completeness of information provided, overall priorities, extent of tailoring required and funding. Note: Use or tailoring of an approved RI will reduce potential engineering and evaluation timelines and effort required.

(b) Complete engineering and evaluation (Step 2 and 3) within 9-12 weeks for connection requirements requiring development of new cross-domain solution. Actual timelines for completion will depend on completeness of information provided, complexity of the proposed new solution, overall priorities, and funding. Note: This is least preferred solution for time-sensitive requirements due to potential engineering and evaluation effort required and unforeseen technical problems.

(c) DSWAG, Flag Panel and DISN DAA will: Approve connection within 1-3 weeks depending level of approval required (DSAWG, Flag Panel, or DISN DAA), completion of engineering and evaluation steps and time sensitivity of request. Note: Approval process coordination can be run concurrently with Step 2 and 3 for high priority (time sensitive) connection requirements, but engineering and evaluation steps must still be completed prior to final approval.

Figure C-1. Connection Process (SIPRNET)



3. NIPRNET Connection Requests

a. Step 0: Prepare Request. C/S/A review connection requirement and prepare information for completing NIPRNET connection request or waiver. See Connection Approval Process (CAP) electronic form on NIPRNET CAP website for information required (HTTP://cap.nipr.mil//).

b. Step 1: Process Request.

(1) Requesting Organization will:

(a) Register NIPRNET connection, by completing the CAP online form, which is submitted electronically via the NIPRNET CAP website (HTTP://cap.nipr.mil//).

(b) Register an Internet Waiver/User Enclave Waiver (reference p), by completing the Internet Waiver/User Enclave Waiver form, which is submitted electronically via the NIPRNET CAP website.

1. An INTERNET waiver is required for temporary approval for a DOD Service or Agency to connect to the Internet and the NIPRNET.

2. A User Enclave Waiver is required for a connection to the Internet by a DOD Service or Agency that is not connected to the NIPRNET.

(2) NIPRNET Connection Approval Office (NCAO) will:

(a) Ensure appropriate validation of each non-DOD request.

(b) Determine type of connection request. Connection types:

1. Routine connection. If the connection is a routine connection NCAO, move directly to step 3.

2. Internet Waiver/User Enclave Waiver.

(c) Evaluate the data for completeness and security relevance.

c. Step 2: Evaluate Waiver

(1) NCAO will:

(a) Facilitate the community security evaluation organizations (e.g. DISA, NSA, and DIA) in performing security evaluations and risk

assessments of waiver.

(2) Ensure security components meet the security criteria (ensure organization evaluation).

(3) NIPRNET PAT will:

(a) Review security evaluations and risk assessments.

(b) Forward connection recommendations to the appropriate approval bodies (DSAWG, Flag Panel, and DISN DAAs).

d. Step 3: Connection Approval

(1) Routine connection.

(a) NCAO will:

1. Notify the requesting organization/user about its approval to connect to the NIPRNET.

2. Send organization a Registration Tracking number and Consent to Monitor form. The Registration Tracking number is necessary for you to make any future changes or updates to the CAP.

(b) Requesting organization will:

1. Sign the Consent to Monitor form (must be signed by the organization's commander, DAA, or other command-designated official).

2. Fax the Consent to Monitor form to (703) 882-2885 or mail signed form to:

DISA, NIPRNET CAP
NS 523 5275
Leesburg Pike Falls Church, VA 22041

(2) Internet Waiver/User Enclave Waiver

(a) NCAO will: Review entire request and other related documentation and provides guidance to the connection approval authorities.

(b) DSAWG will: Review and approve waiver (as delegated) approval or forward recommendations to the Flag Panel.

(c) Flag Panel will: Review and approve waiver (as delegated) or forward recommendation to DISN DAAs for final resolution.

(d) DISN DAAs will: Review and approve waiver. The DISN DAAs may delegate authority to the Flag Panel, DSAWG or NCAO for some waiver decisions.

e. Step 4: Disconnection

(1) NCAO will:

(a) Inform the DISN Flag Panel via the DSAWG of site non-compliance.

(b) Notify the site and the appropriate C/S/A representative.

(c) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the NCAO advises the J6, Joint Staff.

(2) Flag Panel will: Recommend to Joint Staff/J6 that a disconnect warning notice be issued.

(3) Joint Staff will:

(a) Initiate coordination with J3 and enclave component to assess operational impact of the potential disconnects.

(b) Release a message giving 30 days to bring the connection into compliance or submit a plan to achieve connection compliance. Submitted plan must lead to compliance within 60 days of notification message release.

(c) Issue a coordinated DISN DAA order to disconnect, if compliance is not achieved within 30 day or 60 day windows.

(4) DISA network operators. Verify and implement disconnection as directed.

(5) Site DAA. Terminate connection, if DAA determines that a connection is no longer required and notify the DISA SCAO via routine letter/message.

4. Points of contacts

a. Site DAA submits SIPRNET connection requests through GIAP web site (HTTP://giap.disa.smil.mil//).

Site DAA submits NIPRNET connection requests through the NIPRNET CAP website (HTTP://cap.nipr.mil//).

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

VALIDATION AND APPROVAL REQUEST FOR CROSS-DOMAIN, NON-GOVERNMENT, CONTRACTOR OR FOREIGN ENTITY CONNECTIONS

1. Connection requests for DOD cross-domain, Non-DOD government (federal, state, local), contractor or foreign entity connections require validation and approval of operational requirement. This validation and approval request must be submitted before or simultaneously with connection request through GIAP.

2. DOD Cross-Domain Connection. The following connections validation and approval requirements are mandatory for cross-domain connection requirement to SIPRNET of other DOD US classified security domain or unclassified enclaves/networks.

a. Sponsoring organization endorses the connection validation request (see subparagraph 5 for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J6 validates and approves the connection request.

c. Joint Staff, J-6 informs DISA SCAO of validation and approval of operational requirement.

3. Foreign Connection. Following connection validation and approval requirements are mandatory for direct or indirect connections between US classified enclaves and foreign entity. This includes US classified enclaves to US classified enclaves, which permit direct foreign access or connections of US classified enclaves to US enclaves, which are connected to other shared classified enclaves (e.g., coalition, bilateral).

a. Sponsoring DOD C/S/A organization prepares the connection validation request (see subparagraph 5 for Request Example) and forwards to appropriate Combatant Command.

b. Combatant Command reviews and endorses sponsoring organization (Service, or Defense Agency) connection request. If foreign entity country is not located in Combatant Command AOR appropriate Combatant Command will be provided information copy of request. Combatant Command forwards request to Joint Staff, J-6.

c. Joint Staff, J-6 validates and approves connection request.

d. Joint Staff, J-6 informs DISA SCAO of validation and approval of operational requirement.

e. Sponsoring DOD organization is responsible for ensuring compliance with all DOD IA and CND policies and procedures.

4. Non-DOD Government Connection. The following connections validation and approval requirements are mandatory for connections between DOD and Non-DOD government information systems.

a. Sponsoring organization endorses the connection validation request (see subparagraph 5 for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J6 validates the connection request and forwards to ASD(C3).

c. ASD(C3) approves the connection request and informs Joint Staff, J-6.

d. Joint Staff, J-6 informs DISA SCAO of validation and approval of operational requirement.

e. Non-DOD USG organization must comply with all DOD IA and CND policies and procedures.

5. Contractor Connection. The following connection validation and approval requirements are mandatory for connections between DOD and Contractor information systems:

a. Sponsoring DOD organization endorses the connection request (see subparagraph 5 for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J-6 validates the connection request and forwards to ASD(C3).

c. ASD(C3) approves the connection request and informs Joint Staff, J-6.

d. Joint Staff, J-6 informs DISA SCAO of validation and approval of operational requirement.

e. Contractor must comply with all DOD IA and CND policies and procedures.

f. Sponsoring DOD organization agency is responsible for ensuring funding is arranged for the connection.

g. Connection must be physically segregated from the corporate infrastructure.

h. Government sponsor conducts annual on-site security reviews.

6. Memorandum Example. The following memorandum is provided as an example request with required information for connection of Non-DOD USG, contractor or foreign access. The memorandum should be sent to the Joint Staff, J-6, ATTN: J-6T, Washington, D.C. 20318-6000.

EXAMPLE

Defense Threat Reduction Agency
45045 Aviation Drive
Dulles, VA 20166-7517

14 Dec 02

FROM: DTRA-SWET

MEMORANDUM FOR: Joint Staff/ J6T (Attn: Major David Phillips, Room 1D770)

SUBJECT: Secret Internet Protocol Network (SIPRNET) Connectivity for the Federal Emergency Management Agency (FEMA)

1. CONNECTION REQUIREMENT: Request a T-1 SIPRNET connection at FEMA's office in Raliegh, NC and their two of our alternate operating locations in Salem, Oregon and Miami, Florida to support the Integrated Munitions Effects Assessment (IMEA) program.

2. DISCUSSION: The Defense Threat Reduction Agency (DTRA) has developed a tool to aid the weaponeer in defeating high value targets containing weapons of mass destruction. The tool, IMEA, was developed to fill a need arising from the Gulf War. It is fast running and capable of running on a portable, relatively low-end machine. Our customer base has grown to nearly 300 users worldwide since the product's first release three years ago. This year we will be installing a web page on the SIPRNET to allow users to post problem

EXAMPLE

EXAMPLE

reports, communicate with the developer, and obtain other information to facilitate warfighter use. FEMA has been tasked to trouble-shoot and resolve user problems on a real-time basis, and, if needed, to operate 24 hours per day in a help-desk mode. It is, therefore, essential that they have access to the SIPRNET at these three locations to support DTRA.

3. MISSION PARTNERS AND OPERATIONAL JUSTIFICATION:

a. DOD Sponsor Unit: DTRA

b. DOD Sponsor Mission: Provide weaponeering solution with IMEA in support of the warfighter. Develop and analyze crisis planning and provide critical problem resolution support in near real time.

c. Non-DOD agency/Contractor: FEMA

d. Non-DOD agency/Contractor DOD operational requirement:

(1) Secure Development – There will be times when the weaponeer will need assistance in developing a weaponeering solution with IMEA. In crisis planning especially, quick resolution of problems will be critical. In order to assist the user in a timely manner, FEMA may ask them to send us their work via the SIPRNET for analysis. We will provide advice to the user. If problems reside in the programming code, FEMA will develop and distribute the fix via the SIPRNET.

(2) Exercise Support – FEMA and DTRA routinely supports CINC exercises throughout the world. As in crisis planning, there may be problems encountered while trying to weaponeer a target. Problems may involve techniques to model complex targets or developing unique work-around to compensate for unusual situations. Our office is best suited to provide the modeling support, to analyze programming problems, and to develop fixes.

e. Project/Contract # and expiration: SIPRNET access for IMEA is required for four years until 30 Dec 2007.

EXAMPLE

EXAMPLE

4. CONNECTION LOCATION(S):

a. FEMA HQ, 1234 Kitty Hawk Blvd, Raleigh, NC 28817

b. FEMA Detachment 51, 5000 Mountain Drive, Salem, OR 95801

c. FEMA Detachment 23, 2121 Aquarius Ct, Miami, FL 33521

5. ACCESS REQUIRED:

a. Applications/Databases: IMEA, Intellink-S, and NORTHCOM Website

b. Protocols: Web and Mail

c. Specific IP addresses: 198.99.99.2, 201.87.87.81, and 56.94.84.64

d. DOD Installations: Ft. Meade, MD and HQ SOUTHCOM

6. CONCLUSION: Approval of this request will provide for an efficient and economical way for FEMA to support DTRA and the warfighter in crisis and deliberate planning missions as well as provide for an efficient method to release and update future versions of IMEA.

7. POCs:

a. DOD Sponsor: Point of contact at DTRA is Mr Steve Sipperer, commercial (704) 223-8374, fax (704) 223-9001, e-mail SippereS@dtra.mil.

b. Non-DOD Agency/ Contractor: FEMA representative is Mr. Clint Black, commercial (618) 878-2305, e-mail is Clint.Black@fema.gov.

c. Security: FEMA Information Systems Security Officer (ISSO) is Ms Peggy Palmer, commercial (618) 878-7373, fax (618) 878-8399, e-mail is PalmerPe@fema.gov.

LEON R. DONAHUE, GS-15
Program Manager, Special Weapons Targeting

EXAMPLE

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE C

DISN SECURITY ASSURANCE PROGRAM

1. Background. The DISN Security Assurance program integrates C/S/A and DISA inspection and assistance visit programs to assess DISN security status. DISA will support C/S/As through site visits or remote monitoring and vulnerability assessments.

2. Inspections and Visits

a. Site Inspections/Visits. The program consists of three levels of on-site inspections: compliance inspections, assistance visits, and technical engineering inspections/visits. Organizations will integrate types of inspections/visits described below to determine enclave and connection posture. The inspection assets will range from non-technical teams with a systemic orientation to highly technical oriented teams. Examples of assets to conduct on site inspections are Inspectors General (IG), Cross-Domain, and various assistance teams.

(1) Compliance Inspections. Compliance inspections include organizations/team (e.g., C/S/A Inspector General, auditors and DSS) that provide a systemic perspective of several aspects of information assurance; and provide local accrediting authorities a basis for immediate improvement.

(a) Compliance inspections are performed during scheduled visits.

(b) The primary focus is on documentation and the synchronization between local information and centralized repositories maintained by C/S/A and DISN network operators; training and certification deficiencies; network and enclave documentation and systemic issues.

(2) Assistance Visits. Assistance Visits include organizations/teams (e.g., C/S/A IA organizations and DSS) able to identify and evaluate more complex security issues, and, along compliance visit results, provide basis for assessing Information Assurance training, implementation, and operation.

(a) Assistance visits support C/S/A respective Information Assurance programs, the Services and Agencies conduct assistance

visits.

(b) Assistance teams are more technically focused. The teams provide assistance in correcting deficiencies noted by compliance teams, conduct assessment of operational procedures and practices, and evaluate documentation and information handling. The primary focus is to identify and resolve deficient operational practices and procedures as well as device configuration issues.

(c) Assistance teams validate previous compliance inspection results and assist in resolving remaining deficiencies. Repository synchronization will also be accomplished. Unresolved training and certification deficiencies will be noted for resolution within Service and Agency channels.

(3) Technical Engineering Inspections. Technical Engineering inspections include organizations/teams (e.g., C/S/A teams, Cross-Domain Team (formerly SABI Team) and SIPRNET Inspection Team) that provide assurance that trusted devices continue to be maintained and operated in a manner that minimizes community risk, and provide training where necessary.

(a) Technical Engineering inspections (e.g., JVAP) primarily focus on the secure engineering, implementation, and, where applicable, operation of devices that move information across classification boundaries.

(b) Teams validate previous compliance inspections and assistance visit results and resolve remaining deficiencies where possible.

3. Remote Monitoring and Vulnerability Assessments. Remote monitoring and vulnerably assessments develop a profile of potential configuration vulnerabilities and to alert the site. Remote monitoring and vulnerability assessments begin when an enclave is first granted connectivity.

a. C/S/As conduct remote monitoring of enclave and long-haul network operations.

b. Organization providing local and long-haul component will conduct monitoring.

c. Sampling. Sampling is conducted to evaluate quality of service, determine service efficiency, or support engineering actions to improve

network performance.

d. Security. Security assessments will examine consistency of site topology documentation and the conformance of network resident devices with vulnerability alerts issued by DOD CERT. The long-haul operator will accomplish this for the secure networks (JWICS, SIPRNET), and the Services/Agencies will accomplish for NIPRNET.

4. Inspection Criteria

a. Sample checklists for self-assessments and compliance inspections/visits can be found at web site http://guides.ritchie.disa.mil. The checklists cover both traditional security and information assurance.

b. Site visit inspections should follow published criteria for the respective C/S/A or criteria for the particular devices when classification boundaries are involved. Criteria will be established during the initial accreditation of the device.

c. The criteria for remote monitoring will be based on published Secure Technical Implementation Guides (STIGs), vulnerability notices issued through CERT channels, or other criteria established by the C/S/A organization conducting the monitoring and provided to monitored sites.

5. Reporting

a. Inspection/visit findings and results will be published through existing command and technical management channels.

b. Results reporting for contractors will be to the contract management organization, the contract sponsor, and to long-haul network operator(s) and the supporting information assurance management organization of contractor sponsor.

c. Connection documentation formats should be modified to provide an opportunity for an enclave to report when last inspected and the type of inspection, including self-assessments.

6. Enclave Categorization. Criteria for categorizing an enclave are provided in subparagraph 8. This categorization will support allocating limited technical assets to enclaves having the greatest IA benefit for interconnected community as a whole. Additionally, categorization will be used to establish inspection scope and periodicity (subparagraph 7).

7. Inspection Responsibility and Frequency Table. "DISN Networks Security Inspection Table" (Table C-B-1) summarizes the execution concept for the DISN Security Assurance Program.

	NIPRNET		SIPRNET	
Category	Frequency	Inspecting Element	Frequency (Minimum)	Inspecting Element
1	Every 3 Years	IG	Every 3 Years	IG
2	Every 3 Years	C/S/A	Every 3 Years	C/S/A
3 (DOD)	Every 2 Years	C/S/A	Every 2 Years	C/S/A
3 (Contractor)	Annual	DSS	Annual	DSS
4	Annual	C/S/A	Annual	DISA

Table C-B-1. DISN Networks Security Inspection Table

8. Enclave Inspection Categories. The following categories will be applied to connected enclaves as a means to allocate scarce technical inspection assets. Categories reflect enclave configurations that potentially impact enclave/network security posture. The categories accommodate who will accomplish the inspection/visit, the criteria used, and the frequency of inspection/visit. Unless specifically referenced the category criteria for apply to both NIPRNET and SIPRNET enclaves.

a. Category One

(1) Enclave operates at a single classification level.

(2) Enclave employs a firewall or firewall-like device in place between local area network and wide area network.

(3) Enclave does not support remote access.

(4) Internet service is via DISA-provided gateway for NIPRNET connected enclaves.

(5) No cross-domain connections exist for connected enclaves.

b. Category Two

(1) Enclave operates at a single classification level.

(2) Enclave has a firewall in place.

(3) Internet service is via DISA-provided gateway for NIPRNET connected enclaves.

(4) NIPRNET enclave with central dial-in/dial-out modem banks.

c. Category Three

(1) Enclave operates at a single classification level.

(2) NIPRNET enclave with connection to Internet with no firewall or firewall not via DISA-provided gateway.

(3) Contractor facility with NIPRNET connectivity.

(4) SIPRNET enclave without firewalls.

(5) SIPRNET enclave that supports a central dial-in/dial-out modem bank.

d. Category Four

(1) Any enclave that has cross-domain connections that move information between two different classification levels (includes foreign systems).

(2) Contractor site with SIPRNET connectivity.

(3) Any site with non-US personnel integrated into work force/work area with SIPRNET access.

(4) Any site that is identified by the DISA SCAO as non-compliant in providing requested connection approval documentation, or does not meet the compliance timeline in a failed DISA SCAO remote network assessment.

9. Joint Vulnerability Assessment Process (JVAP)

a. All sites with an approval to connect to the DISN are subject to an annual on-site JVAP, or as otherwise directed by the Joint Staff.

b. The JVAP is a process using checklists and DISA and NSA procedures to assess specific configurations, operations and administration of the cross-domain solution(s).

c. Types of JVAPS

(1) Scheduled JVAP. Scheduled JVAPs will be performed annually and will be coordinated and scheduled in advance with the local/site DAA and the site POC.

(2) Short Notice JVAP. Short notice JVAPs will be performed as required. This may occur with limited (less than 24 hours) notification and coordination with the local/site DAA and POC.

d. The JVAP verifies the configuration and identifies possible security vulnerabilities of a cross-domain solution. A cross-domain solution connects two domains and restricts the information that transfers between the domains. The security posture and operations of the cross-domain solution must be in compliance with approved conditions to maintain connection authorization.

e. A DISA Field Security Office team lead will notify the local/site DAA and the C/S/A representative for both scheduled and short notice JVAP visits. In cases when the local/site DAA is not available, the C/S/A representative will be asked to assist in the coordination of the visit.

f. DISA and NSA will perform data collection and analysis on the cross-domain solution(s). The collection and analysis will result in a detailed listing of vulnerabilities with recommended corrective actions. The results are maintained in a secure database by DISA. The site will be responsible for updating status of corrective action through the local/site DAA. The final report, to include recommended corrective action(s), will be made available to the local/site DAA.

g. High-risk vulnerabilities will be corrected (when possible) prior to the JVAP team leaving the site. The status of remaining vulnerabilities will be reported by the local/site DAA until closed.

ENCLOSURE D

REFERENCES

a. CJCSI 6250.01, Series, “Satellite Communications”

b. CJCSI 6215.01, Series, “Policy for Department of Defense Voice Networks”

c. DCID 6/3, Series, “Protecting Sensitive Compartmented Information within Information Systems”

d. DODI 4640.14, 6 December 1991, "Base and Long-Haul Telecommunications Equipment and Services"

e. DOD Directive 8500.1, Series, “Information Assurance (IA)”

f. DOD Instruction 5200.40, 30 December 1997, ”DOD Information Technology Security Certification and Accreditation (C&A) Process”

g. DOD 8510.1-M, 31 July 2000, “DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual”

h. DOD 5200.1-R, 14 January 1997, “Information Security Program”

i. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

j. CJCSI 5221.01, Series, “Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations”

k. DOD Instruction 8500.2, Series, “Information Assurance (IA) Implementation”

l. CJCSI 6510.01, Series, “Information Assurance (IA) and Computer Network Defense (CND)”

m. DISA Circular 310-130-4, 18 August 1993, “Defense User’s Guide to the Telecommunications Service Priority (TSP) System”

n. CJCSM 6510.01, Series, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)"

o. NSTISSI No. 7003, 13 December 1996, "Protected Distribution System"

p. ASD (C3I) Memorandum, 22 August 1999, "Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)"

q. Defense Information System Network (DISN) Long-Haul Block Security Policy, May 1999

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

A

AOR	area of responsibility
ASD(C3)	Assistant Secretary of Defense Command, Control, and Communications
ATC	Authority to Connect

C

C/S/A	Combatant Command, Service and Defense Agency
C4I	command, control, communications, computers and intelligence
CAP	connection approval process
CDSO	Cross-Domain Solutions Organization
CDTAB	Cross-Domain Technical Advisory Board
CIO	Chief Information Officer
CISA	Communication Information Service Activity
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COMSEC	communications security
COP	common operational picture
CTF	coalition task force

D

DAA	Designated Approving Authority
DBOF	Defense Business Operating Fund
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DICAST	Defense and Intelligence Community Accreditation Support Team
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DRSN	Defense Red Switch Network
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service

	G
GIAP	GIG interconnection approval process
GIG	Global Information Grid
	I
IA	information assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAPB	Information Assurance Policy Board
IATC	interim authority to connect
IAW	in accordance with
IC	Intelligence Community
IG	Inspector General
ISSE	information systems security engineering
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	information technology
	J
JTF	joint task force
JVAP	Joint Vulnerability Assessment Process
JWICS	Joint Worldwide Intelligence Communications system
	M
MCEB	Military Communication Electronics Board
	N
NCAO	NIPRNET Connection Approval Office
NIPRNET	Non-classified Internet Protocol Router Network
NSA	National Security Agency
NSEP	National Security Emergency Preparedness
	O
OSD	Office of the Secretary of Defense
	P
PAT	process action team
PDS	protected distribution system
	R
RI	referenced implementation
	S
SABI	SECRET and Below Interoperability
SAP	special access program

SAR	Special Access Requirement
SCAO	SIPRNET Connection Approval Office
S_C_I	sensitive compartmented information
SIPRCAP	SIPRNET Connection Approval Process
SIPRNET	SECRET Internet Protocol Router Network
SSAA	System Security Authorization Agreement
STIGs	Secure Technical Implementation Guides

T

TSABI	TOP SECRET and Below Interoperability
TSP	Telecommunications Service Priority

U

USSTRATCOM	US Strategic Command

V

VMS	Vulnerability Management System

PART II--DEFINITIONS

accreditation. Formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

certification. Comprehensive evaluation of the technical and non-technical security safeguards of IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Common Criteria. The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (IT) security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Community. Data and system owners who are affiliated by information system interconnection.

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

connection approval. Formal authorization to interconnect information systems.

cross-domain solution. An information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains.

data. An object (e.g., file, set of files, information, imagery, graphics) that is developed, assembled, and packaged by a producer for transfer across security domains.

Defense Information System Network (DISN). The DOD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations

designated approving authority (DAA). Responsible for weighing the security risks of operating an automated information system versus the benefits it may provide and deciding whether or not to approve operation of the system.

DISN user. An individual assigned to an organization having devices directly or indirectly connected to the DISN.

DISN Security Accreditation Working Group (DSAWG). Provides, interprets, and approves DISN security policy, guides architecture development, and recommends accreditation decisions to the DISN Flag panel.

DOD CIO Executive Board Charter for Adjudication of Requests for Waiver of DISN. The DOD CIO Executive Board is the single DOD executive level providing senior management recommendations and decision support for adjudication of requests for waiver of the DISN. The board is supported by the GIG Waiver Review Panel.

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DOD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

Defense Intelligence Community Accreditation Support Team (DICAST). Supports the intelligence principal accreditation authorities (PAAs), which includes, the Director of the NSA, the Director of the DIA, the Director of the NRO, or the Executive Director of the Central Intelligence Agency. The responsibilities of the DICAST are outlined in DCID 6/3 (reference c).

enclave. An environment under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer.

End-to-End. The fusion of all requisite components to deliver a defined capability. For the GIG, this implies all components from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For the DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone).

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

GIG Interconnection Approval Process. Electronic process to submit connection information and register a GIG connection.

guards. Process limiting the exchange of information between systems.

interconnected. An *interconnected* information is composed of *separately accredited* information systems (i.e., Enclaves). Each self-contained information system maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating information system has its own IAO (ISSO).

information assurance. Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Joint Vulnerability Assessment Process (JVAP). A process using checklists and DISA/NSA procedures to assess specific configurations, operations and administration of the cross-domain solution(s).

Protection Profile. A protection profile contains a set of security requirements either from the Common Criteria for Information Technology Security Evaluation (CCITSE), or stated explicitly, which should include an Evaluation Assurance Level (EAL). The protection profile permits the implementation independent expression of security requirements for a set of Targets of Evaluation (TOEs) that will comply fully with a set of security objectives.

referenced implementation (RI). An approved interconnection security implementation maintained by the NSA and made available for reuse or for use as a guide.

Risk Decision Authority Criteria. Criteria for identifying an acceptable level of community risk appropriate for the connection approval authorities to employ in making connection decisions.

robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DOD has three levels of robustness:

high robustness. Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

medium robustness. Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

low robustness. Security services and mechanisms that equate to good commercial practices.

security domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.

security markings. Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions. For DOE information, these could include indicators of information type (such as Restricted Data), and Sigma categories.

security penetration testing. System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain "root" or "superuser" privileges) by exploiting flaws in system design or implementation.

subnetwork. A logical partition of a network amenable to separate management, control, and provisioning because of functional or geographic reasons.

system. A generic term for a collection of equipment connected to the DISN. It may refer to a host, a group of hosts, or a network.

validation. The confirmation, by designated authority, that a request for access and use of the DISN is necessary to meet that organization's mission requirements.